Politika e Privatësisë dhe Siguria e Klientit

I. Politika e Privatësisë

Në këtë dokument jepet një informacion i detajuar në lidhje me administrimin dhe përpunimin e informacionit dhe të dhënave personale të përdoruesve që vizitojnë faqen e internetit të Union Bank. Me hyrjen në këtë faqe interneti apo me plotësimin e çdo aplikimi online, përdoruesi deklaron se jep miratimin e tij për procesimin e mëtejshëm të informacionit nga ana e Union Bank.

Faqja **www.unionbank.al** është faqja zyrtare në internet e Union Bank sh.a.

Union Bank mbledh të dhëna me karakter personal të përdoruesve (subjektet e të dhënave personale) të cilat regjistrohen në sistemet e saj apo të ofruesve të tjerë të shërbimeve të autorizuar prej saj. Në këtë faqe, përdoruesi mund të hasë në forma të ndryshme aplikimi, si aplikimet e produktit "Dua Kredi", aplikime për punë, akses në shërbimet online, aplikim për ankesa të ndryshme etj.
Të gjithë formularet apo e-mail-et e dërguara me dëshirë në adresën e bankës e specifikuar në këtë faqe interneti përfshin marrjen në vijim të adresës së dërguesit që nevojitet për t'ju përgjigjur kërkesave të tij duke përfshirë edhe çdo të dhënë tjetër personale të domosdoshme mbi procesin apo shërbimin e kërkuar. Gjithashtu mund të regjistrohet edhe IP e kompjuterit të përdoruesit.

Union Bank thekson se ofrimi i të dhënave personale të përdoruesve nëpërmjet plotësimit të formularëve të ndryshëm nuk është i detyrueshëm dhe është në dëshirën e çdo subjekti për të dhënë vullnetarisht informacionin e kërkuar për të krijuar dhe vijuar me tej marrëdhenien e biznesit me përdoruesit. Në rast se përdoruesi nuk pranon të vërë në dispozicion të bankës këto të dhëna, banka mund të refuzojë lidhjen e një kontrate, ose nuk do të jetë në gjendje të vazhdojë ekzekutimin e një kontrate ekzistuese, ose mund të jete e detyruar të ndërprese këtë kontratë në vijim.

Përdoruesit duhet të vënë në dispozicion të bankës ato të dhëna që kërkohen të mblidhen bazuar në ligjet në fuqi apo rregullore të ndryshme. Përpunimi i të dhënave personale mund të kryhet edhe ne rastet e përmbushjes së detyrimeve të ndryshme ligjore për bankat, për Parandalimin e Pastrimit të Parave, për Taksat, për ekzekutimin e Vendimeve Gjyqësore etj. Kur është e nevojshme, të dhënat e perdoruesve përpunohen edhe për të mbrojtur interesat e ligjshme të Bankës ose të palëve të treta.

Union Bank siguron përdoruesit (subjektet e të dhënave personale) se të dhënat e tyre mblidhen dhe përpunohen vetëm për qëllime të realizimit të marrëdhënies bankare duke marrë të gjitha masat fizike, teknike, operacionale me standard të lartë sigurie për ruajtjen e konfidencialitetit si dhe mbrojtjen nga humbja, shkatërrimi, dëmtimi apo edhe shpërndarja e paautorizuar, në

përputhje me kërkesat e Ligjit Nr.9887, datë 10.3.2008, ''Për mbrojtjen e të dhënave personale'' përgjatë gjithë marrëdhënies bankare dhe në vijimësi. Në rast se Union Bank duhet t'ua transmetojë të dhënat e mbledhura palëve të treta (partnerë të saj në biznes), Banka siguron subjektet se këto të dhëna përdoren vetëm për qellimin e realizimit të shërbimit bankar për qëllimin për të cilin përdoruesi ka deklaruar vullnetarisht të dhënat e tij personale. Në këto raste Union Bank siguron përdoruesit se kontratat e lidhura me të tretët për këtë qëllim janë të qarta dhe në to parashikohen kushtet e sigurisë dhe ruajtjes së konfidencialitetit.

Bazuar në ligjin Nr. 9887 datë 10.03.2008 përdoruesi – subjekt i të dhënave personale, në çdo moment pasi të ketë dhënë vullnetarisht informacionin e kërkuar, i lind e drejta që, nëpërmjet një kërkese pranë Union Bank, të aksesojë këto të dhëna, të verifikoje saktësinë e tyre si dhe të kërkoje korrigjimin apo edhe përditësimin e tyre duke u bazuar plotësisht në nenin 13 te ligjit nr. 9887.

Theksojmë se bazuar në nenin 16 të Ligjit nr. 9887, datë 10/03/2008 "Për Mbrojtjen e të Dhënave Personale", përdoruesi (subjekti i të dhënave personale) gëzon të drejtën e ankimit në rast se pretendon se i janë shkelur të drejtat, liritë dhe interesat e ligjshëm në lidhje me të dhënat personale. Në rast se subjekti i të dhënave ka bërë ankim, Banka nuk do të kryejë ndryshime në të dhënat e tij personale deri në dhënien e vendimit. Kërkesat duhet të drejtohen në adresën **info@unionbank.al** ose dërgohen në adresë të bankës:

Union Bank, Njësia Administrative nr. 9, Sheshi "Ferenc Nopçka" Kodi Postar 1016, Nr. i ndërtesës 5, Tiranë, Shqipëri.

Ankesat nga përdoruesit (subjekte të të dhënave personale) mund të adresohen me e-mail edhe pranë Komisionerit për Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale në adresën e mëposhtme: **info@idp.al**

Të dhënat personale ruhen për aq kohë sa është e nevojshme për marrëdhënien e biznesit me bankën në përputhje me detyrimin për ruajtje bazuar në Kodin Civil, Ligjin për Arkivat, Ligjin për Parandalimin e Pastrimit të Parave, etj.

Në funksion të informimit të përdoruesve të kësaj faqe interneti për çdo përdorues të saj, Banka ka publikuar në vijim elementet e sigurisë së aplikuar në disa nga produktet e saj (Kartat, UB Online).

I. Privacy Policy

This document provides detailed information regarding the administration and processing of information and personal data of users visiting Union Bank's website. By accessing this website or completing any online application, the user declares that he/she gives his/her approval for further processing of the information by Union Bank.

www.unionbank.al is the official website of Union Bank sh.a.

Union Bank collects personal data of users (personal data subjects) which are registered in its systems or other service providers authorized by it. On this site, the user can encounter various application forms, such as applications for the product "Dua Kredi", job applications, access to online services, application for various complaints, etc.
All forms or e-mails sent voluntarily to the bank's address specified on this website include recording the sender's address needed to respond to his/her requests as well as any other personal information which is considered necessary for the process or service required. The IP of the user's computer can also be recorded.

Union Bank emphasizes that providing users personal data through the completion of various forms is not mandatory and is up to every user to voluntarily provide the information required to establish and maintain further the business relationship. In case the user refuses to make this data available to the bank, the bank may refuse to enter into a contract agreement, or will not be able to continue the execution of an existing contract, or may be obliged to terminate this contract agreement.

Users must make available to the bank the data required to be collected based on applicable laws or various regulations. The processing of personal data can also be performed in cases of fulfilling various legal obligations for banks, for the Prevention of Money Laundering, for Taxes, for the execution of Judicial Decisions, etc. When necessary, user's data are also processed to protect the legitimate interests of the Bank or third parties.

Union Bank assures users (personal data subjects) that their data is collected and processed only for the purpose of attaining the banking relationship by taking all physical, technical, operational measures with high security standards to maintain confidentiality and protection from loss, destruction, damage or even unauthorized distribution, in accordance with the requirements of Law No. 9887, dated 10.3.2008, "On the protection of personal data" throughout the banking relationship and onwards. In case Union Bank has to transmit the collected data to third parties (its business partners), the Bank assures the users that this data is used only for the purpose of performing the banking service for which the user has voluntarily declared his/her personal data. In these cases, Union Bank assures users that the contracts with third parties for this purpose are clear and they reflect the terms of security and confidentiality.

Based on law no. 9887 date 10.03.2008 the user - personal data subject, at any moment after having voluntarily provided the requested information, through a request to Union Bank, has the

right to access this data, to verify their accuracy and request their correction or even update based on Article 13 of Law no. 9887.

We emphasize that based on Article 16 of Law no. 9887, dated 10/03/2008 "On the Protection of Personal Data", the user (personal data subject) has the right to complain if he/she claims that his/her rights, freedoms and legitimate interests related to the personal data have been violated. In case the personal data subject has filed a complaint, the Bank will not make changes to his personal data until the decision is issued. Requests should be directed to **info@unionbank.al** or sent to the Bank's address:

Union Bank, Njësia Administrative nr. 9, Sheshi "Ferenc Nopçka" Kodi Postar 1016, Nr. i ndërtesës 5, Tiranë, Shqipëri

The complaints from users (personal data subjects) can also be addressed by e-mail to the Information and Data Protection Commissioner at the following address: **info@idp.al**

Personal data is stored for as long as is necessary for the business relationship with the bank, in accordance with the safekeeping obligation based on the Civil Code, the Law on Archives, the Law on Prevention of Money Laundering, etc.

In order to inform the users of this website, the Bank has published the following security elements applied in some of its products (Cards, UB Online).

II. Siguria e Klientit

➢ Siguria e Kartave

Investimet e Union Bank në drejtim të mbrojtjes së klientëve nga përdorimi i të dhënave të kartave nga persona të pa-autorizuar:

- Migrimi i kartave në teknologjinë Chip rrit sigurinë në përdorimin e kartave për transaksionet që kryhen kur karta është fizikisht prezente. Eshtë shumë e vështirë për t'u kryer kopjimi i të dhënave nga karta Chip.
- Për të mbrojtur klientët tanë nga rreziku i marrjes së të dhënave të kartës nga persona të pa-autorizuar për veprimet ku karta nuk është prezente (p.sh veprimet në internet), Union Bank ka investuar në implementimin e autentifikimit 3D-secure (Mastercard Secure Code).
- Union Bank njofton klientin duke derguar SMS për çdo transaksion që kryhet me kartën e kreditit.
- Union Bank ofron shërbimin Internet Banking nëpërmjet të cilit mund të kontrolloni online veprimet e kryera me kartë.
- Për t'i shërbyer sa më mirë dhe në çdo kohë klientëve të saj, Union Bank ka vënë në shërbim Call Center ku mund të kontaktoni në çdo moment që mund t'ju nevojitet për të bllokuar kartën tuaj.
- Banka i ofron mundësinë klientëve të zgjedhin limitin e vlefshëm të dëshiruar për përdorim në Internet, duke siguruar kështu uljen e ekspozimit nga rrezikut i mashtrimit.

Për të shmangur përdorimin dhe marrjen e të dhënave të kartës nga persona të pa-autorizuar Ju këshillojmë:

- Të nënshkruani kartën në pjesën e pasme të saj, menjëherë sapo të merrni kartën në dorëzim.
- Asnjëherë mos mbani në të njëjtin vend Kartën dhe PIN-in. Union Bank ju sygjeron të memorizoni PIN-in dhe me pas të shkatërroni fletën e PIN-it.
- Gjatë vendosjes së PIN-it, sigurohuni që askush tjetër nuk është duke e vëzhguar atë.
- Siguroni që karta të jetë nën vëzhgimin tuaj gjatë gjithë kohës kur jeni duke kryer pagesë me të.
- Gjatë kryerjes së një transaksioni në internet, siguroni se keni aksesuar një site të certifikuar SSL (https).
- Ndiqni me kujdes veprimet e kryera me kartë të shfaqura në llogarinë tuaj ose në faturën e kartës së kreditit. Nëse konstatoni veprime të cilat nuk janë kryer nga ju, kontaktoni menjeherë bankën.
- Në rast humbje, vjedhje të kartës, kontaktoni menjeherë Call Center të Union Bank për të kryer bllokimin e kartës.

➢ Siguria e UB Online

Kërkesa për sigurinë mbi shërbimet bankare të lëvizshme

Përdorimi i një smartphone/tableti për të manaxhuar financat tuaja është një mjet i shkëlqyer që ju ofron mundësinë të monitoroni dhe të përdorni paratë tuaja praktikisht kudo që të jeni. Pavarsisht kësaj, ju duhet të aplikoni disa kërkesa shtesë që të përdorni shërbimet elektronike bankare në mënyrë të sigurtë.

Siguroni paisjen/telefonin e zgjuar (smartphone)

Me ndihmën e një kodi hyrës apo nëpërmjet shënjes së gishtit, ju duhet të rrisni sigurinë e smartphone/tabletit tuaj të zgjuar gjatë përdorimit. Sigurimi i paisjes suaj do të rrisë gjithashtu mbrojtjen për aplikacionin tuaj bankar, veçanërisht në rastet kur telefoni mund t'ju humbasë apo vidhet. Informoni menjëherë operatorin tuaj të telefonisë së lëvizshme në rastet kur telefoni ju humbet/vidhet për të kërkuar bllokimin e numrit dhe bllokimin e paisjes në rast se kjo e fundit ofrohet. Kur jeni në ambjente publike sigurohuni që paisja të jetë nën vëzhgimin tuaj gjithmonë. Kyçeni paisjen kur nuk e përdorni.
Gjithashtu njoftoni menjëhere Bankën të bllokoni shërbimin UB Online në rast se keni aktivizuar Soft Token në smatphone/tabletin tuaj në rast se ky i fundit humbet/vidhet.

Siguroni fjalëkalimin/kodin PIN

Përdorni fjalëkalim/kod PIN të fortë. Mos përdorni numra në radhë, numrat e datë lindjeve apo numrat e kartës së identitetit, apo kombinime të tilla gjatë krijimit të fjalëkalimit. Mos ruani asnjëherë fjalëkalime apo kode PIN të shërbimeve bankare në paisjen tuaj celulare. Nëse telefoni humbet ose sulmohet kjo do të rrisë shanset që ju të bini pre e kriminelëve kibernetikë. Fjalëkalimin/kodin PIN mos e ndani me të tjerë.

Kontrolloni aplikacionin/faqen përpara se ta shkarkoni

Sigurohuni që ju shkarkoni aplikacionin e bankës dhe çdo lloj aplikacioni tjetër të rëndësishem për ju, vetëm nga dyqanet zyrtare të prodhuesëve (si janë App Store ose Play Store). Duhet të jeni dyshues për çdo aplikacion të ri jo-familjar. Në disa raste ata mund të përmbajnë viruse që lehtësojnë hyrjen në të dhëna sensitive. Gjithashtu, kontrolloni herë pas here nëse aplikacionin e bankës suaj e keni të përditësuar. Versionet e vjetra të aplikacioneve bankare mund të kenë mekanizma sigurie të papërditësuar.
Sigurohuni që aksesoni shërbimin bankar gjithmonë nga faqja zyrtare e bankës në rastet kur aksesoni shërbimin nga interneti.

Përdorni rrjete të sigurta dhe të besueshme për lidhjen

Ne ju rekomandojmë të mos lidheni me rrjete publike Wi-Fi dhe të ç'aktivizoni funksionin e Bluetooth përpara se të hyni në aplikacionin tuaj bankar. Edhe nëse përdorni një rrjet privat Wi-

Fi sigurohuni që është i siguruar me sistemin WPA2. Ju këshillojmë të instaloni programe anti-virus të përditësuara.

Siguroni transaksionet tuaja

Kontrolloni në kohë periodike llogarinë tuaj. Nëse vini re ndonjë tërheqje apo transfertë jo të zakonshme reagoni menjëherë duke kontaktuar bankën.

Mesazhet ''Phishing''

Jini të vëmendshëm ndaj telefonatave, mesazhe të postës elektronike apo mesazhe tekst të pakërkuara. Këto mesazhe ''phishing'' përmbajnë kërkesa të tipit me urgjence ose të tipit të ofertave të mahnitshme që do t'ju kërkojnë që të dhënat tuaja sensitive tu jepen mashtruesëve. Trajtojini këto mesazhe me skepticizëm. Mos jepni asnjëhere informacione personale. Banka nuk do t'ju kërkojë asnjëherë të jepni fjalëkalimin apo kodin PIN.

Siguroni kompjuterin

Mbroni kompjuterin tuaj nga viruse të ndryshme duke përdorur antiviruse të liçensuar dhe të përditësuar. Sigurohuni që kompjuteri është i paisur me "Firewall" i cili ju mbron nga përdorues të paautorizuar për të parandaluar vjedhjen e të dhënave personale.

Elemente Sigurie

Çfarë bën Banka për mbrojtjen e informacionit konfidencial të klienteve të UB Online? Shërbimi UB Online i Union Bank përfshin të gjithë komoditetin që ju duhet për të sjelle bankën më pranë jush me teknologjine më të fundit dhe të sigurtë të kohës për mbrojtjen e të dhënave tuaja.

Akses i sigurtë i llogarive

Shërbimi UB Online ofron teknologjinë më të lartë të enkriptimit 2048 -bit SSL Secure Socket Layer. Kjo teknologji mbron të dhënat tuaja në 2 mënyra:

1. Enkriptimi, nënkupton që të dhënat e shkëmbyera me bankën nuk mund të lexohen nga persona të pautorizuar.
2. "Integriteti i të dhënave", nënkupton që të dhënat që ju shkëmbeni me anë të programit UB Online nuk modifikohen nga persona të pautorizuar.

Për të rritur nivelin e sigurisë Banka ofron pajisje të sigurisë së lartë Smart Token për autentikimin në shërbimin UB Online. Këto pajisje përdorin One Time Password (kod autentikimi i vlefshëm për një logim të vetëm).

II. Shërbimi ofron mundësinë e përdorimit të tastieres virtuale për vendosjen e detajve të sigurisë.

II.Customer Security

➢ Cards Security

Union Bank investments for protecting customers from the use of cards data by unauthorized persons:

- Card migration in Chip technology increases the security of using the card for transactions that take place when the card is physically present. It is very difficult to copy data from the Chip card.
- To protect our customers from the risk of unauthorized persons receiving card's data for transactions where the card is not present (e.g. online transactions), Union Bank has invested in the implementation of 3D-secure authentication (Mastercard Secure Code).
- Union Bank sends SMS notifications for every transaction performed with the credit card.
- Union Bank offers Internet Banking service through which you can check online the transactions performed with the card.
- In order to better serve to its customers at any time, Union Bank has set up a Call Center service which you can contact at any time when you need to block your card.
- The bank offers to the customers the opportunity to choose the desired available limit for Internet use, thus ensuring reduced exposure to fraud risk.

To avoid the use from unauthorized persons receiving card's data, we advise you to:

- Sign the card on the back as soon as you receive the card.
- Never keep your Card and PIN in the same place. Union Bank suggests that you memorize the PIN and then destroy the envelope containing it.
- When entering the PIN, make sure no one else is watching.
- Ensure that the card is under your observation at all times when you are making payments with it.
- When performing an online transaction, make sure you have access to an SSL certified site (https).
- Carefully track card transactions displayed on your account or credit card bill. If you notice any transaction that have not been performed by you, contact the bank immediately.
- In case of loss, theft of the card, contact immediately the Call Centre of Union Bank to block the card.

➢ UB Online Security

Security requirements on mobile banking services

Using a smartphone / tablet to manage your finances is a great tool that offers you the ability to monitor and use your money virtually wherever you are. Nevertheless, you need to apply some additional requirements to use electronic banking services safely.

Secure your device / smartphone

With the help of a password or fingerprint, you need to increase the security of your smartphone / tablet while using it. Securing your device will also increase the protection for your banking application, especially in cases where your phone may be lost or stolen. Inform your mobile operator immediately in case your phone is lost / stolen requesting to lock your SIM card and device if this is offered. When you are in public places make sure the device is always under your supervision. Lock the device when not in use.

Also, immediately notify the Bank to block the UB Online service in case you have activated the Soft Token on your smartphone / tablet in case it is lost or stolen.

Provide password / PIN code

Use a strong password / PIN code. Do not use consecutive numbers, date of birth or ID card numbers, or any such combinations when creating a password. Never store bank passwords or PINs on your mobile device. If the phone is lost or attacked this will increase the chances of you falling prey to cyber criminals. Do not share your password / PIN with others.

Check the app / site before downloading

Make sure you download the bank's app and any other app important to you, only from the manufacturer's official stores (such as the App Store or Play Store). You should be skeptical of any new non-familiar app. In some cases, they may contain viruses that facilitate access to sensitive data. Also, check from time to time if your bank's application is up to date. Older versions of banking applications may have outdated security mechanisms.

Make sure that you always access the banking service from the official website of the bank in case you access the service from the internet.

We recommend that you do not connect to public Wi-Fi networks and turn off the Bluetooth function before accessing your banking application. Even if you use a private Wi-Fi network make sure it is secured with the WPA2 system. We advise you to install updated anti-virus programs.

Use secure and reliable networks for connection

We recommend that you do not connect to public Wi-Fi networks and turn off the Bluetooth function before accessing your banking application. Even if you use a private Wi-Fi network make sure it is secured with the WPA2 system. We advise you to install updated anti-virus programs.

Check your account periodically. If you notice any unusual withdrawals or transfers, react immediately by contacting the bank.

Phishing messages

Beware of unsolicited phone calls, e-mails or text messages. These "phishing" messages contain urgent requests or amazing offers that will require you to disclose your sensitive information to fraudsters. Treat these messages with skepticism. Never give out personal information. The bank will never ask you to provide a password or PIN.

Protect your computer from various viruses by using licensed and up-to-date antivirus software. Make sure your computer is equipped with a Firewall that protects you from unauthorized users to prevent personal data theft.

Security elements

What does the Bank do to protect the confidential information of UB Online customers?
Union Bank's UB Online service includes all the convenience you need to bring your bank closer to you with the latest and most secure technology for protecting your data.

Secure account access

UB Online service offers the highest encryption technology 2048 -bit SSL Secure Socket Layer.

This technology protects your data in 2 ways:

1. Encryption, means that the data exchanged with the bank cannot be read by unauthorized persons.
2. “Data integrity” means that the data you exchange through the UB Online program is not modified by unauthorized persons.

To increase the level of security, the Bank offers high security devices “Smart Token” for authentication in the UB Online service. These devices use One Time Password (valid authentication code for a single login).
The service offers the possibility of using the virtual keyboard for entering security details.